



Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at <http://about.jstor.org/participate-jstor/individuals/early-journal-content>.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

On the Asymptotic Value of Sums of Power Residues.*

BY HOWARD H. MITCHELL.

1. In this paper certain limits will be obtained for the sum of all the positive integers less than a given prime m , the indices of which, with respect to a primitive root of m have the same residue, mod 2ν , where 2ν is a divisor of $m-1$. If $(m-1)/2\nu$ is even, $\text{ind } (m-r) \equiv \text{ind } r, \text{ mod } 2\nu$, and hence the value of a sum of the type mentioned is $m(m-1)/4\nu$. We shall therefore suppose that $(m-1)/2\nu$ is odd.

By means of the limits obtained for these sums it will be found that if S_i denotes any one of them, and if ν remains fixed while m ranges over the primes that are congruent to $2\nu+1, \text{ mod } 4\nu$,† then

$$\lim_{m \rightarrow \infty} \left[\frac{\frac{S_i}{m(m-1)}}{\frac{1}{4\nu}} \right] = 1.$$

Perhaps the most interesting result that has been established concerning the sums of the type considered is that if m be a prime of the form $4n+3$ the sum of the quadratic non-residues of m that lie between 0 and m always exceeds the sum of the residues. From this it follows that the number of the residues between 0 and $m/2$ exceeds the number of the non-residues. These results were established by Dirichlet in connection with his investigation of the class number of quadratic forms.‡

Stern has shown that if m is a prime of the form $8n+3$, the sum of the quadratic non-residues between 0 and m is less than twice the sum of the residues, whereas if it has the form $8n+7$, the sum of the non-residues is less than three times the sum of the residues.§ The latter result, however, is

* Presented to the American Mathematical Society, December 28, 1916.

† Dirichlet has shown that in any arithmetical progression in which the first term and common difference have no common factor there is an infinity of primes (Dirichlet-Dedekind, *Zahlentheorie*, 4th edition, §§ 132-137).

‡ *Ibid.*, § 104.

§ *Journal für Mathematik*, Vol. LXXI (1870), pp. 152, 153; Bachman, *Encyklopädie der Mathematischen Wissenschaften*, Bd. I, p. 569.

trivial, since in whatever way the integers from 1 to $m-1$ be divided into two sets containing $(m-1)/2$ numbers each, the sum of either set is less than three times the sum of the other.

The distribution of the quadratic residues is a problem that is closely related to the values of these sums, and one that has interested a number of writers.*

2. The author's results concerning the sums of the sort described are obtained by use of a certain type of Dirichlet's series. These series are special cases of those that were used in his proof of the infinity of primes in an arithmetical progression.† They were also employed by Kummer in the derivation of the expression for the class number of a cyclotomic realm.‡

Following the notation of Dirichlet–Dedekind,§ we write

$$L^{\circ}(\alpha) = \sum_z \frac{\alpha^{\text{ind } z}}{z},$$

where the sum is to be taken over all the positive integers z that are not divisible by a given prime m , α denotes any root of the equation $\alpha^{\nu} = -1$, where 2ν is a divisor of $m-1$, and $\text{ind } z$ denotes the index of z , mod m , with respect to a particular primitive root.

In case $(m-1)/2\nu$ is odd, the sum of this series may be expressed in finite form as follows:||

$$L^{\circ}(\alpha) = -\frac{\pi i}{m^2}(\alpha, \theta)\phi(\alpha).$$

The symbol (α, θ) denotes the Lagrange resolvent function

$$(\alpha, \theta) = \sum_{r=1}^{m-1} \alpha^{\text{ind } r} \theta^r,$$

where $\theta = e^{2\pi i/m}$. The symbol $\phi(\alpha)$ is defined by

$$\phi(\alpha) = -\sum_r r \alpha^{-\text{ind } r},$$

where r assumes the same values.

* Lebesgue, *Journal de Mathématiques*, Vol. VII (1842), p. 137; Götting, *Journal für Mathematik*, Vol. LXX (1869), p. 363; Stern, *loc. cit.*; Osborn, *Messenger of Mathematics*, Vol. XXV (1895), p. 45; Glaisher, *Quarterly Journal of Mathematics*, Vol. XXXIII (1902), pp. 319–328; *ibid.*, Vol. XXXIV (1903), pp. 1, 178; Karpinski, *Journal für Mathematik*, Vol. CXXVII (1904), p. 1; Holden, *Messenger of Mathematics*, Vol. XXXV (1905), pp. 102, 110; *ibid.*, Vol. XXXVI (1906), pp. 75, 126.

† *Loc. cit.*; also Werke, Vol. I, p. 313.

‡ *Journal für Mathematik*, Vol. XL, p. 98.

§ P. 625.

|| Combining equations (58), (65), *loc. cit.*

We proceed to obtain an upper limit for the absolute value of $L^\circ(\alpha)$. In consequence of our assumption that $(m-1)/2\nu$ is odd, the series may be written in the form*

$$L^\circ(\alpha) = \sum_r \alpha^{\text{ind } r} \left[\frac{1}{r} - \frac{1}{m-r} + \frac{1}{m+r} - \frac{1}{2m-r} + \dots \right],$$

where the sum is to be taken over the positive integers r that are less than $m/2$. The absolute value of $L^\circ(\alpha)$ is thus less than

$$1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{\frac{m-1}{2}} < \log\left(\frac{m+1}{2}\right) + C,$$

where C denotes Euler's constant, $C = .577 +$.

The absolute value of (α, θ) is equal to \sqrt{m} . Hence the absolute value of $\phi(\alpha)$ is less than

$$\frac{m\sqrt{m}}{\pi} \left[\log\left(\frac{m+1}{2}\right) + C \right].$$

The function $\phi(\alpha)$ may be written in the form

$$\phi(\alpha) = - \sum_{i=0}^{2\nu-1} S_i \alpha^{-i},$$

where S_i denotes the sum of the positive integers r less than m for which $\text{ind } r \equiv i, \text{ mod } 2\nu$. Since we are assuming that $\alpha^\nu = -1$, this may in turn be written

$$\phi(\alpha) = \sum_{i=0}^{\nu-1} (S_{i+\nu} - S_i) \alpha^{-i}.$$

From this we obtain

$$\nu(S_{i+\nu} - S_i) = \sum_a \alpha^i \phi(\alpha),$$

where the sum is to be taken over all the roots of the equation $\alpha^\nu = -1$, and where i may have any one of the values $0, 1, 2, \dots, \nu-1$.

We therefore conclude that

$$|S_{i+\nu} - S_i| < \frac{m\sqrt{m}}{\pi} \left[\log\left(\frac{m+1}{2}\right) + C \right].$$

If a number r appears in the sum S_i , then $m-r$ will appear in the sum $S_{i+\nu}$, and hence

$$S_{i+\nu} + S_i = \frac{m(m-1)}{2\nu}.$$

The values of S_i and $S_{i+\nu}$ are thus included between the limits,

$$\frac{m(m-1)}{4\nu} \pm \frac{m\sqrt{m}}{2\pi} \left[\log\left(\frac{m+1}{2}\right) + C \right].$$

* Cf. Glaisher, *Quarterly Journal of Mathematics*, Vol. XXXIII (1902), pp. 306, 307, 317.

From this it is clear that these sums obey an asymptotic law in that if ν is considered to remain fixed, and m to range over the primes that are congruent to $2\nu+1$, mod 4ν , then

$$\lim_{m \rightarrow \infty} \left[\frac{S_i}{\frac{m(m-1)}{4\nu}} \right] = 1.$$

3. Certain extensions of these results are possible in case m is composite. For example, if m is an odd integer of the form $4n+3$ not divisible by a square factor, and $\left(\frac{z}{m}\right)$ denotes the Jacobi symbol for quadratic residues, we have*

$$\sum_z \left(\frac{z}{m}\right) \frac{1}{z} = -\frac{\pi}{m\sqrt{m}} \sum_r \left(\frac{r}{m}\right) r,$$

where the sum on the left is to be taken over all the positive integers z that are prime to m , and the sum on the right over all the positive integers r that are less than m and prime to m .

From this relation we obtain in the same manner as above

$$-\sum \left(\frac{r}{m}\right) r < \frac{m\sqrt{m}}{\pi} \left[\log \left(\frac{m+1}{2} \right) + C \right],$$

from which we conclude that the sum of the positive integers r that are less than and prime to m , and for which $\left(\frac{r}{m}\right) = +1$ is included between the limits

$$\frac{m\phi(m)}{4} - \frac{m\sqrt{m}}{2\pi} \left[\log \left(\frac{m+1}{2} \right) + C \right], \quad \frac{m\phi(m)}{4},$$

and the sum of those for which $\left(\frac{r}{m}\right) = -1$ is included between the limits

$$\frac{m\phi(m)}{4}, \quad \frac{m\phi(m)}{4} + \frac{m\sqrt{m}}{2\pi} \left[\log \left(\frac{m+1}{2} \right) + C \right],$$

where, as usual, $\phi(m)$ denotes the number of integers less than and prime to m .

If e is any fixed number less than 1, it may be shown that if m be taken sufficiently large, $\phi(m) > m^e$. From this it follows that

$$\frac{m\phi(m)}{4}$$

is an asymptotic value for either of the two sums.

A similar generalization may be given in the case of higher residues.

4. By means of the above result we may obtain an upper limit for the number of classes of quadratic forms of determinant $-m$, where m is an odd integer of the form $4n+3$ not divisible by a square factor. This number is given by

$$h = -\frac{1}{m} \left[2 - \left(\frac{2}{m} \right) \right] \Sigma \left(\frac{r}{m} \right) r,^*$$

and it therefore satisfies the inequality,

$$h < \left[2 - \left(\frac{2}{m} \right) \right] \frac{\sqrt{m}}{\pi} \left[\log \left(\frac{m+1}{2} \right) + C \right].$$

For large values of m this is a much lower limit than those obtained by Holden;† in fact it is evident that if e denotes any fixed number greater than $1/2$,

$$\lim_{m \rightarrow \infty} \left[\frac{h}{m^e} \right] = 0.$$

Similar results may be obtained for the number of classes of ideals in the quadratic realm $k(\sqrt{-m})$.‡

By means of the upper limit found in § 2 for the absolute value of the function $\phi(\alpha)$ an upper limit may also be obtained for the so-called *first factor* of the class number of the cyclotomic realm determined by m -th roots of unity. § Kummer has stated, apparently without proof, that this first factor obeys an asymptotic law. ||

An upper limit may also be obtained for the first factor of the class number of the realm of degree 2ν , determined by the 2ν periods formed from m -th roots of unity, where $(m-1)/2\nu$ is odd.¶

UNIVERSITY OF PENNSYLVANIA, PHILADELPHIA, PA.

* Dirichlet–Dedekind, § 104.

† *Messenger of Mathematics*, Vol. XXXV (1905), p. 106.

‡ Hilbert, “Die Theorie der algebraischen Zahlkörper,” *Jahresbericht der Deutschen Mathematiker-Vereinigung*, Vol. IV (1894), p. 320.

§ Kummer, *Journal für Mathematik*, Vol. XL (1850), p. 110; Dirichlet–Dedekind, p. 630.

|| *Journal de Mathématiques*, Vol. XVI (1851), p. 473. Cf. also H. J. S. Smith, “Report on the Theory of Numbers,” *Works*, Vol. I, p. 114.

¶ Kummer, *Journal für Mathematik*, Vol. XL (1850), p. 112.